xatla AG Business Software
Dorfmattweg 8a | 3110 Münsingen
+41 31 331 01 01 | info@xatla.ch

Auftragsverarbeitungsvertrag

1 Gegenstand

Dieser Vertrag regelt die Rechte und Pflichten der xatla AG als Auftragnehmerin und der Auftraggeberin, einer Kundin der xatla AG (nachfolgend gemeinsam die «**Parteien**») im Zusammenhang mit der datenschutzrechtlichen Auftragsbearbeitung beziehungsweise Auftragsverarbeitung (nachfolgend einheitlich die «**Auftragsverarbeitung**») von Personendaten beziehungs-weise personenbezogenen Daten (nachfolgend einheitlich die «**Personendaten**»).

Mit diesem Vertrag ermöglicht die Auftragnehmerin der Auftraggeberin die Einhaltung der anwendbaren datenschutzrechtlichen Anforderungen für die Auftragsverarbeitung.

Dieser Vertrag ist für alle Tätigkeiten anwendbar, bei denen die Auftragnehmerin ganz oder teilweise Personendaten im Auftrag der Auftraggeberin bearbeitet beziehungsweise verarbeitet oder bearbeiten beziehungsweise verarbeiten (nachfolgend einheitlich «**verarbeiten**») lässt.

Die Auftragnehmerin unterliegt dem schweizerischen Datenschutzrecht, insbesondere gemäss dem Bundesgesetz über den Datenschutz (DSG). Die Europäische Kommission stellte mit Entscheidung vom 26. Juli 2000 fest, dass das schweizerische Datenschutzrecht ein angemessenes Schutzniveau für Personendaten gewährleistet. Die Feststellung gilt als Angemessenheitsbeschluss gemäss Art. 45 Abs. 1 der europäischen Datenschutz-Grundverordnung (DSGVO).

2 Art, Gegenstand und Zweck der Auftragsverarbeitung

Die Auftragsverarbeitung erfolgt gemäss bestehenden oder noch zu schliessenden vertraglichen Vereinbarungen zwischen den Parteien wie insbesondere Allgemeinen Geschäftsbedingungen (AGB). Die Bestimmungen dieses Vertrages haben Vorrang bei einem Widerspruch zwischen den Bestimmungen dieses Vertrages und sonstigen vertraglichen Vereinbarungen zwischen den Parteien.

Die Auftragsverarbeitung umfasst jeden Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Abfragen, Abgleichen, Anpassen, Archivieren, Aufbewahren, Auslesen, Bekanntgeben, Beschaffen, Einschränken, Erfassen, Erheben, Löschen, Offenlegen, Ordnen, Organisieren, Speichern, Verändern, Verknüpfen, Vernichten und Verwenden von Personendaten. Personendaten sind alle Angaben, die sich auf eine bestimmte oder bestimmbare beziehungsweise identifizierte oder identifizierbare natürliche Person beziehen, deren Daten verarbeitet werden.

Die Auftragsverarbeitung umfasst die Kategorien von Personendaten gemäss **Anhang 1**.

Die Auftragsverarbeitung umfasst die Kategorien betroffener Personen, deren Personendaten verarbeitet werden, gemäss **Anhang 2**.

3 Pflichten der Parteien

3.1 Weisungen und Zweckbindung

Die Auftragnehmerin verarbeitet Personendaten ausschliesslich für den Zweck beziehungsweise die Zwecke gemäss den vertraglichen Vereinbarungen zwischen den Parteien oder gemäss dokumentierten Weisungen der Auftraggeberin, es sei denn, die Auftragnehmerin ist gesetzlich oder regulatorisch zu einer bestimmten Verarbeitung verpflichtet. Die Auftraggeberin kann während der gesamten Dauer der Auftragsverarbeitung weitere dokumentierte Weisungen erteilen.

Die Auftragnehmerin informiert die Auftraggeberin, wenn sie eine erteilte Weisung ganz oder teilweise nicht ausführen kann. Die Auftragnehmerin informiert die Auftraggeberin, wenn sie der Auffassung ist, dass vertragliche Vereinbarungen oder erteilte Weisungen gegen anwendbare datenschutzrechtliche Anforderungen verstossen.

3.2 Sicherheit

Die Auftragnehmerin ergreift mindestens die geeigneten technischen und organisatorischen Massnahmen (TOM) gemäss **Anhang 3**, um eine dem Risiko angemessene Sicherheit der verarbeiteten Personendaten (nachfolgend die «**Datensicherheit**») zu gewährleisten. Diese Massnahmen umfassen insbesondere den Schutz der verarbeiteten Personendaten, darunter allenfalls auch besonders schützenswerte Personendaten, vor einer Verletzung der Datensicherheit.

12 Die Auftragnehmerin gewährt ihren Hilfspersonen nur insoweit Zugang zu Personendaten der Auftraggeberin, als ein solcher Zugang für die Durchführung, Überwachung und Verwaltung dieses Vertrages erforderlich ist. Die Auftragnehmerin gewährleistet, dass sich die zur Auftragsverarbeitung befugten Personen zur Geheimhaltung verpflichtet haben oder einer angemessenen gesetzlichen Geheimhaltungspflicht unterliegen.

3.3 Dokumentation und Prüfmöglichkeiten

Die Parteien müssen die Einhaltung dieses Vertrages nachweisen können.

Die Auftragnehmerin bearbeitet in angemessener Weise und möglichst zeitnah Anfragen der Auftraggeberin zur Auftragsverarbeitung gemäss diesem Vertrag.

Die Auftragnehmerin stellt der Auftraggeberin auf Anfrage alle vorhandenen Informationen zur Verfügung, die für den Nachweis der Einhaltung der in diesem Vertrag festgelegten und unmittelbar aus den anwendbaren datenschutzrechtlichen Bestimmungen hervorgehenden Anforderungen erforderlich sind.

Die Auftragnehmerin ermöglicht der Auftraggeberin auf Verlangen die Prüfung der Auftragsverarbeitung gemäss diesem Vertrag in angemessenen Abständen oder bei dokumentierten Anzeichen für eine Nichteinhaltung.

Die Auftraggeberin kann eine solche Prüfung selbst durchführen oder durch eine unabhängige Prüferin beziehungsweise einen unabhängigen Prüfer durchführen lassen. Solche Prüfungen sind auf einen Tag pro Kalenderjahr beschränkt. Eine Prüfung kann auch Inspektionen in den physischen Einrichtungen oder Räumlichkeiten der Auftragnehmerin umfassen, sofern solche Inspektionen erforderlich sind, zu den üblichen Geschäftszeiten ohne Störung des Betriebsablaufs stattfinden und die Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit er-folgt. Solche Inspektionen sind im Übrigen nur zulässig, sofern und soweit die Prüfung nicht durch geeignete Nachweise wie beispielsweise Bestätigungen, Dokumentationen und Zertifikate oder Zertifizierungen erfolgen kann, insbesondere bei Rechenzentren.

Die Auftraggeberin trägt die Kosten der Auftragnehmerin für solche Prüfungen.

Die Parteien stellen einer zuständigen Aufsichtsbehörde beziehungsweise zuständigen Aufsichtsbehörden die oben genannten Informationen, einschliesslich Ergebnissen von Prüfungen, auf Anfrage zur Verfügung, sofern die Zurverfügungstellung nicht aus gesetzlichen Gründen verboten ist.

4 Unterauftragsverarbeitung

Die Auftraggeberin erteilt der Auftragnehmerin die allgemeine Genehmigung für die Beauftragung von Unterauftragsverarbeitern, die in der Liste gemäss **Anhang 4** aufgeführt sind.

Die Auftragnehmerin unterrichtet die Auftraggeberin mindestens 30 Tage im Voraus in elektronischer oder schriftlicher Form über alle beabsichtigten Änderungen dieser Liste durch Ersetzen oder Hinzufügen von Unterauftragsverarbeitern. Die Auftragnehmerin räumt der Auftraggeberin damit ausreichend Zeit ein, um vor der Beauftragung allfällige Einwände gegen die beabsichtigten Änderungen erheben zu können.

Erfolgt kein fristgerechter Widerspruch, gelten die beabsichtigten Änderungen als genehmigt. Ist bei einem Widerspruch keine einvernehmliche Klärung zwischen den Parteien über die geplanten Änderungen möglich und ist die Auftraggeberin nicht bereit, auf ihren Widerspruch zu verzichten, sind die Parteien berechtigt, diesen Vertrag ausserordentlich auf den Zeitpunkt der geplanten Änderungen zu kündigen.

Die Auftragnehmerin muss Unterauftragsverarbeitern, die zur Durchführung der Auftragsverarbeitung beauftragt werden, vertraglich im Wesentlichen die gleichen Pflichten auferlegen wie diejenigen, die für die Auftragnehmerin gemäss diesem Vertrag gelten. Die Auftragnehmerin stellt sicher, dass jeder Unterauftragsverarbeiter die Pflichten erfüllt, denen die Auftragnehmerin gemäss diesem Vertrag und gemäss den anwendbaren datenschutzrechtlichen Anforderungen unterliegt.

5 Export von Personendaten

Jeder Export von Personendaten in ein Land ausserhalb der Schweiz und der Mitgliedstaaten des Europäischen Wirtschaftsraumes (EWR) oder an eine internationale Organisation erfolgt aus-schliesslich wie vertraglich vereinbart oder gemäss dokumentierten Weisungen der Auftraggeberin, es sei denn, die Auftragnehmerin ist gesetzlich zu einem bestimmten Daten-Export verpflichtet. In einem solchen Fall informiert die Auftragnehmerin die Auftraggeberin über diese gesetzliche Verpflichtung, sofern eine solche Information nicht aus gesetzlichen Gründen verboten ist.

Jeder Export von Personendaten in ein Land ausserhalb der Schweiz und der Mitgliedstaaten des EWR erfolgt grundsätzlich ausschliesslich, wenn das Datenschutzrecht im jeweiligen Land gemäss dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) beziehungsweise dem Schweizerischen Bundesrates ein angemessenes Schutzniveau für Personendaten gewährleistet.

Der Export von Personendaten in ein Land ausserhalb der Schweiz und der Mitgliedstaaten des EWR, dessen Datenschutzrecht kein angemessenes Schutzniveau von Personendaten gewährleistet, darf ausnahmsweise erfolgen, wenn aus anderen Gründen ein angemessenes Schutzniveau gemäss den anwendbaren datenschutzrechtlichen Anforderungen gewährleistet ist, insbesondere gemäss zwischenstaatlichen Vereinbarungen oder auf Grundlage von geltenden Standardvertragsklauseln, die von der Europäischen Kommission erlassen wurden. Die Auftrag-nehmerin ist berechtigt, solche europäischen Standardvertragsklauseln gemäss Empfehlungen des EDÖB so anzupassen und zu ergänzen, dass die Standardvertragsklauseln auch den an-wendbaren datenschutzrechtlichen Anforderungen in der Schweiz entsprechen und damit geeignet sind, ein angemessenes Datenschutzniveau beim Daten-Export aus der Schweiz zu gewährleisten.

Die Beauftragung von Nylas Inc., USA, als Unterauftragsverarbeiter erfolgt unter Anwendung der Standarddatenschutzklauseln der Europäischen Kommission gemäss Empfehlung des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB). Eine Kopie der geltenden Garantien kann auf Anfrage zur Verfügung gestellt werden.

6 Unterstützung der Auftraggeberin

Die Auftragnehmerin informiert die Auftraggeberin unverzüglich über jeden datenschutzrechtlichen Antrag, den sie von einer betroffenen Person erhalten hat, und der die Auftragsverarbeitung betrifft. Die Auftragnehmerin ist berechtigt, der betroffenen Person den Erhalt zu bestätigen, beantwortet den Antrag im Übrigen aber nicht selbst, es sei denn, sie wurde von der Auftraggeberin damit beauftragt.

Die Auftragnehmerin unterstützt die Auftraggeberin unter Berücksichtigung der Art der Auftragsverarbeitung bei der Erfüllung ihrer Pflicht, datenschutzrechtliche Anträge betroffener Personen zu beantworten.

Die Auftragnehmerin unterstützt die Auftraggeberin ferner unter Berücksichtigung der Art der Auftragsverarbeitung und der vorhandenen Informationen bei der Einhaltung der folgenden Pflichten:

- Führung eines allfälligen Verzeichnisses der Verarbeitungstätigkeiten;
- Durchführung einer Datenschutz-Folgenabschätzung, wenn eine geplante Verarbeitung von Personendaten durch die Auftraggeberin voraussichtlich ein hohes Risiko für die Grundrechte oder die Persönlichkeit der betroffenen Personen mit sich bringen kann;
- Konsultation der zuständigen Aufsichtsbehörde(n) vor der Verarbeitung von Personendaten, wenn eine Datenschutz-Folgenabschätzung ergibt, dass die geplante Verarbeitung trotz der vorgesehenen Massnahmen ein hohes Risiko für die Grundrechte oder die Persönlichkeit der betroffenen Personen mit sich bringt.

Die Auftraggeberin trägt die Kosten der Auftragnehmerin für diese Unterstützung.

7 Meldung von Verletzungen der Datensicherheit

Die Auftragnehmerin arbeitet im Fall einer Verletzung der Datensicherheit mit der Auftraggeberin zusammen. Die Auftragnehmerin unterstützt die Auftraggeberin bei der Erfüllung ihrer Pflichten zur Meldung von Verletzungen der Datensicherheit an die zuständige(n) Aufsichtsbehörde(n) beziehungsweise zur Benachrichtigung der von Verletzungen der Datensicherheit betroffenen Personen, wobei die Auftragnehmerin die Art der Auftragsverarbeitung und die ihr zur Verfügung stehenden Informationen berücksichtigt.

Die Auftraggeberin trägt die Kosten der Auftragnehmerin für diese Unterstützung.

8 Aussetzung der Auftragsverarbeitung

Für den Fall, dass die Auftragnehmerin ihren Pflichten gemäss diesem Vertrag nicht nachkommt, kann die Auftraggeberin die Auftragnehmerin anweisen, die Auftragsverarbeitung auszusetzen, bis die Auftragnehmerin diesen Vertrag einhält oder dieser Vertrag beendet ist. Die Auftragnehmerin informiert die Auftraggeberin unverzüglich, wenn sie – aus welchen Gründen auch immer – nicht in der Lage ist, diesen Vertrag einzuhalten.

9 Haftung

Die Haftung richtet sich nach einer allfälligen Haftungsregelung gemäss den vertraglichen Vereinbarungen zwischen den Parteien.

10 Dauer und Kündigung

Die Auftragnehmerin verarbeitet Personendaten auf unbestimmte Zeit bis zur Kündigung der letzten vertraglichen Vereinbarung zwischen den Parteien, die eine Auftragsverarbeitung betrifft.

Die Auftraggeberin ist berechtigt, diesen Vertrag ausserordentlich und fristlos zu kündigen, wenn:

- die Auftraggeberin die Auftragsverarbeitung ausgesetzt hat und die Einhaltung dieses Vertrages nicht innerhalb einer angemessenen Frist, in jedem Fall aber nicht innerhalb eines Monats nach der Aussetzung, wiederhergestellt wurde;
- die Auftragnehmerin in erheblichem Umfang oder fortdauernd gegen diesen Vertrag verstösst oder die anwendbaren datenschutzrechtlichen Anforderungen nicht erfüllt;
- die Auftragnehmerin der bindenden Entscheidung einer zuständigen Aufsichtsbehörde oder eines zuständigen Gerichts, welche Pflichten der Auftragnehmerin gemäss den an-wendbaren datenschutzrechtlichen Anforderungen zum Gegenstand hat, nicht nach-kommt.

Die Auftragnehmerin ist berechtigt, diesen Vertrag ausserordentlich und fristlos zu kündigen, wenn die Auftraggeberin auf der Erfüllung einer vertraglichen Vereinbarung oder Weisung besteht, nachdem sie von der Auftragnehmerin darüber in Kenntnis gesetzt wurde, dass die vertragliche Vereinbarung oder Weisung gegen anwendbare datenschutzrechtliche Anforderungen verstösst.

Nach Beendigung dieses Vertrages löscht die Auftragnehmerin alle im Auftrag der Auftraggeberin verarbeiteten Personendaten, es sei denn, die Auftragnehmerin ist gesetzlich oder regulatorisch berechtigt oder verpflichtet, die Personendaten zu speichern. Bis zur Löschung der Personendaten gewährleistet die Auftragnehmerin die Einhaltung dieses Vertrages.

11 Schlussbestimmungen

Dieser Vertrag kann in elektronischer oder schriftlicher Form geschlossen werden. Anpassungen dieses Vertrages können in elektronischer Form erfolgen.

Die Parteien informieren sich gegenseitig über eine allfällige Datenschutzberaterin oder über einen allfälligen Datenschutzberater beziehungsweise über eine allfällige Datenschutzbeauftragte oder über einen allfälligen Datenschutzbeauftragten gemäss den anwendbaren datenschutzrechtlichen Anforderungen.

Die Parteien sind verpflichtet, alle im Rahmen dieses Vertrages erlangten Kenntnisse von Geschäftsgeheimnissen der jeweils anderen Partei sowie über Personendaten auch über die Beendigung dieses Vertrages hinaus dauerhaft vertraulich zu behandeln, es sei denn, eine Partei ist gesetzlich zu einer bestimmten Offenlegung verpflichtet. In einem solchen Fall informiert die verpflichtete Partei die jeweils andere Partei über diese gesetzliche Verpflichtung, sofern, solange und soweit eine solche Information nicht aus gesetzlichen Gründen verboten ist. Bestehen bei einer Partei Zweifel, ob eine Information dieser Geheimhaltungspflicht unterliegt, ist die Information bis zur ausdrücklichen Freigabe durch die jeweils andere Partei vertraulich zu behandeln.

Sollten einzelne Bestimmungen dieses Vertrages unerfüllbar, ungültig oder unwirksam sein, so berührt dies die Erfüllbarkeit, Gültigkeit oder Wirksamkeit der übrigen Bestimmungen nicht und die Parteien ersetzen die einzelne Bestimmung mit einer erfüllbaren, gültigen oder wirksamen Bestimmung, die dem angestrebten datenschutzrechtlichen Ergebnis der einzelnen Bestimmung möglichst nahekommt.

Für diesen Vertrag gilt ausschliesslich schweizerisches Recht. Das Kollisionsrecht und das UN Kaufrecht sind ausgeschlossen. Ausschliesslicher Gerichtsstand ist am Sitz der Auftragnehmerin.

Anhang 1 – Kategorien der verarbeiteten Personendaten

Die Auftraggeberin bestimmt und kontrolliert im eigenen Ermessen und in eigener Verantwortung, welche Kategorien von Personendaten verarbeitet werden. Die Auftragsverarbeitung kann insbesondere folgende Kategorien von Personendaten umfassen:

- Anstellungsdaten
- Behandlungsdaten
- E-Mail-Metadaten (z. B. Absender, Empfänger, Betreff, Zeitstempel, etc.)
- Daten zur Intimsphäre
- Daten zum Sozialversicherungsstatus
- Diagnosedaten
- Gesundheitsdaten
- Inhaltsdaten
- Kalenderdaten (z. B. Zeit, Ort, Titel und Teilnehmer von Terminen, etc.)
- Kommunikationsdaten (z. B. E-Mail-Inhalte, Chat-Protokolle, etc.)
- Kontaktdaten
- Medikationsdaten
- Nutzungsdaten
- Reaktionsdaten
- Stammdaten
- Symptombeschreibungsdaten
- Termindaten
- Verordnungsdaten
- Versicherungsdaten
- Vertragsdaten
- Zahlungsdaten
- Zugriffsdaten auf verknüpfte Systeme (z. B. API-Tokens, Authentifizierungsdaten, etc.)

xatla AG Business Software
Dorfmattweg 8a | 3110 Münsingen
+41 31 331 01 01 | info@xatla.ch

Anhang 2 – Kategorien betroffener Personen, deren Personendaten verarbeitet werden

Die Auftraggeberin bestimmt und kontrolliert im eigenen Ermessen und in eigener Verantwortung die Kategorien betroffener Personen, deren Personendaten verarbeitet werden. Die Auftragsverarbeitung kann insbesondere folgende Kategorien von Personendaten umfassen:

- Ansprechpartner
- Ansprechpersonen
- Dienstleistern
- Externe Kontakte aus verknüpften Plattformen oder Diensten
- Gesundheitseinrichtungen
- Geschäftspartner
- Interessenten
- Kundinnen und Kunden
- Kommunikationspartner (z. B. E-Mail- oder Kalenderkontakte)
- Lieferanten
- Mitarbeitende
- Nutzerinnen und Nutzer
- Patientinnen und Patienten

xatla AG Business Software
Dorfmattweg 8a | 3110 Münsingen
+41 31 331 01 01 | info@xatla.ch

Anhang 3 – Technische und organisatorische Massnahmen (TOM)

Die technischen und organisatorischen Massnahmen (TOM) zur Sicherstellung des Schutzes und der Sicherheit der verarbeiteten Personendaten werden aufgeteilt: Die Auftragnehmerin stellt als Herstellerin die Applikation bereit und verantwortet deren Software- und Datenbanksicherheit. Die zugrunde liegende Infrastruktur sowie die Betriebsumgebung werden von der ServerBase AG, Schweiz, als Hosting-Dienstleister bereitgestellt.

Die Auftragnehmerin ist als agiles Schweizer KMU auf die Applikationsentwicklung spezialisiert und verfügt bewusst nicht über eigene, separate ISO-Zertifizierungen, stellt jedoch durch eine professionelle Arbeitsweise sowie die gezielte Auswahl zertifizierter Partner ein hohes Datenschutzniveau sicher. Sie stellt sicher, dass die ServerBase AG alle erforderlichen Massnahmen gemäss den geltenden datenschutzrechtlichen Anforderungen einhält. Die wichtigsten Massnahmen umfassen:

1. **Applikations- und Datenbanksicherheit (Verantwortung Auftragnehmerin)**
    1. **Pentests:** Das von der Auftragnehmerin eingesetzte Software-Framework wird Penetration Tests (Sicherheits-Schwachstellenanalysen) durch externe Spezialisten unterzogen.
    2. **Kontinuierliche Aktualisierung**: Die Applikation wird von der Auftragnehmerin laufend gewartet und mit aktuellen Sicherheits-Patches versorgt.
    3. **Proaktive Überwachung:** Kontinuierliches Monitoring der Applikations-Performance sowie des SQL-Servers, um Anomalien oder unbefugte Zugriffsversuche sofort zu erkennen.
    4. **Kryptografische Trennung & Verschlüsselung (At Rest):** Auf dem Speicher abgelegte Dateien (Files) sowie sensible Datenfelder innerhalb der Datenbank werden standardmässig verschlüsselt gespeichert. Die Entschlüsselung ist strikt auf den jeweiligen Organisationsschlüssel limitiert. Dieser Organisationsschlüssel ist wiederum kryptografisch mit dem individuellen User-Schlüssel verschlüsselt. Ein direkter Zugriff auf Tabellenebene ist ohne die aktive Session des Benutzers technisch unmöglich und die Daten bleiben unlesbar.
2. **Erweiterter Edge-Schutz & Cyber-Abwehr (Myra Security)**
   Der Applikation ist Myra als spezialisierter, dreischichtiger Schutzschirm (HTTP/S-Reverse-Proxy) direkt vorgeschaltet. Die Filterung erfolgt gemäss den Richtlinien der EU-DSGVO. Dies umfasst:
    1. **Hyperscale Web Application Firewall (WAF):** Kontinuierliche Filterung des Traffics auf Inhaltsebene zur Schliessung von Sicherheitslücken und zur Abwehr von Angriffen nach den OWASP Top 10 (z. B. SQL-Injections, Cross-Site Scripting [XSS], Directory Traversal).
    2. **DDoS- & Bot-Schutz:** Permanentes, transparentes Filtern schadhafter Traffic-Ströme (volumen-, infrastruktur- und applikationsbasierte Angriffe). Durch den Einsatz der Myra-Plattform ist der Schutzschirm bedarfsgerecht und hochskalierbar ausgelegt, um selbst grossvolumige Angriffe effektiv abzuwehren, bevor sie die Hosting-Infrastruktur erreichen.
    3. **Multi Site Load Balancer:** Intelligente Lastverteilung des Inbound-Traffics über die Infrastruktur. Integrierte Ausfallerkennung (*Dead Backend Detection / Site Fail Over*) sorgt dafür, dass temporär nicht erreichbare Server automatisch übersprungen werden, um die Hochverfügbarkeit (SLA von mind. 99.9%) zu garantieren.

4. **Automatisiertes Certificate Management:** Sichere Datenübertragung durch erzwungenes HTTPS, Perfect Forward Secrecy (PFS) als Standard, HSTS-Unterstützung sowie vollautomatisierte Ausstellung und rechtzeitige Erneuerung von TLS/SSL-Zertifikaten zur Vermeidung von Sicherheitslücken.

3. **Rechenzentrumsstandorte und Zertifizierungen (Hosting durch ServerBase AG)**
    1. **Schweizer Datenhaltung:** Die Daten werden ausschliesslich in den Schweizer Rechenzentren der ServerBase AG (Rümlang ZH und Lupfig AG) gespeichert und verarbeitet.
    2. **Compliance-Standards:** Diese Infrastruktur ist vollumfänglich nach ISO 27001 zertifiziert und erfüllt die Vorgaben der FINMA (FINMA RS 08/7) sowie das Schweizer Datenschutzgesetz (DSG).
4. **Kontinuierliche Sicherheitsüberwachung (SOC / NOC)**
    1. **24/7-Überwachung:** Die zugrunde liegende Netzwerk- und Serverinfrastruktur wird rund um die Uhr (24/7/365) durch das dedizierte Security Operations Center (SOC) sowie das Network Operations Team (NOC) von Myra überwacht, um IT-Sicherheitsvorfälle in Echtzeit zu erkennen und mittels definierter Eskalationsstufen abzuwehren.
5. **Physische Sicherheitsmassnahmen (ServerBase AG)**
    1. **Zutrittskontrolle:** 24/7-Sicherheitsdienst vor Ort zur Überwachung der Rechenzentren und strenge, mehrstufige Zutrittskontrollen (z. B. biometrische Scans, Ausweiskontrollen) zur Verhinderung unbefugten Zugangs.
    2. **Infrastrukturschutz:** Automatisierte Gaslöschanlagen für den Brandschutz, redundante Stromversorgung (USV/Notstrom) und hochmoderne Klimatisierungssysteme für den optimalen Betrieb der Hardware.
6. **Datensicherung und -wiederherstellung**
    1. **CH-Geo-redundante Backups (Garantierte Schweizer Datenresidenz):** Regelmässige, automatisierte Backups aller Kundendaten zur effektiven Vermeidung von Datenverlust. Da es sich um hochsensible Daten handelt, verbleiben diese zu jedem Zeitpunkt vollumfänglich in der Schweiz. Die verschlüsselten Backups werden räumlich getrennt ausschliesslich in den beiden Schweizer ServerBase-Rechenzentren (Rümlang ZH und Lupfig AG) aufbewahrt.
    2. **Betriebskontinuität**: Erprobte Wiederherstellungsprozesse zur schnellen Datenwiederherstellung bei Störungen (*Disaster Recovery*) sowie proaktive Wartung der IT-Infrastruktur.
7. **Sicherer Kundensupport und Cobrowsing (Fullview)**
    1. **Isoliertes Cobrowsing:** Für den technischen Kundensupport wird die Technologie von **Fullview** eingesetzt. Bei Support-Sitzungen erhält das Support-Team ausschliesslich Einblick in das isolierte Browser-Tab der Web-Applikation. Ein Zugriff auf den restlichen Desktop oder Drittapplikationen des Nutzers ist technisch ausgeschlossen.
    2. **Automatisches Data Masking (Datenschutz-Filter):** Zum Schutz hochsensibler Daten (insb. Patientendaten) ist ein automatischer Datenschutz-Filter aktiv. Sensible Eingabefelder, persönliche Daten oder Passwörter werden für das Support-Personal in Echtzeit **automatisch geschwärzt (maskiert)** und gar nicht erst übertragen.
    3. **Einwilligungsbasiert:** Eine Support-Sitzung kann zu keinem Zeitpunkt unbemerkt gestartet werden; sie erfordert immer die explizite, aktive Freigabe durch den Endnutzer.

8. **Organisatorische Massnahmen & Nachweise**
    1. **Interne Sicherheit der Auftragnehmerin:** Pragmatische und wirksame Rechtevergabe (Need-to-know-Prinzip / Minimalprinzip), konsequente Nutzung von Multi-Faktor-Authentifizierung (MFA) für Systemzugriffe sowie die fortlaufende Sensibilisierung der eigenen Mitarbeitenden im Bereich Datenschutz.
    2. **Dokumentation:** Nachweise über die Infrastruktur (wie ISO 27001-Zertifizierungen der ServerBase AG oder Myra-Sicherheitsberichte) können Kunden auf Anfrage zur Verfügung gestellt werden.

Anhang 4 – Liste der Unterauftragsverarbeiter

Die Auftragnehmerin beauftragt im Zusammenhang mit der Auftragsverarbeitung folgende Unterauftragsverarbeiter:

- **Myra Security GmbH**, Deutschland – Bereitstellung des Content Delivery Networks (CDN), hochentwickelter Sicherheitsdienste (Hyperscale Web Application Firewall) und des Schutzes vor DDoS-Angriffen. Die Datenverarbeitung erfolgt vollumfänglich konform mit den Anforderungen des Schweizer DSG und der EU-DSGVO ausschliesslich auf Infrastruktur innerhalb der Europäischen Union (EU).
- **cloudscale.ch AG**, Schweiz – Bereitstellung digitaler Infrastruktur (Cloud-Hosting und Server-Dienste).
- **Datadog, Inc**., USA – Bereitstellung von Logging- und Monitoring-Diensten (Analyse und Überwachung von IT-Systemen).
- **Health Info Net AG (HIN)**, Schweiz – IT-Lösungen und Vernetzung für das Schweizer Gesundheitswesen (sichere Kommunikation und Datenverarbeitung).
- **Intercom Inc**., USA **/ Intercom R&D Unlimited Company**, Irland – Bereitstellung von Support- und Kommunikationsdiensten (z. B. Chatfunktion, Kundenanfragen, Automatisierung). Die Datenverarbeitung erfolgt auf Grundlage eines abgeschlossenen Data Processing Addendum (DPA) mit Standardvertragsklauseln gemäss Art. 16 Abs. 2 lit. d DSG.
- **LINK Mobility Austria GmbH**, Österreich – Versand und Management von SMS-Nachrichten (Kommunikationsdienstleistungen).
- **MediData AG**, Schweiz – IT-Lösungen für das Schweizer Gesundheitswesen (elektronische Abrechnungs- und Datenübermittlungsdienste).
- **Microsoft Corporation**, USA / **Microsoft Ireland Operations Ltd**. – Bereitstellung von Cloud- und Plattformdiensten (z. B. SignalR, Azure-Komponenten).
- **Nylas Inc**., USA – Bereitstellung von Programmierschnittstellen (APIs) für den Zugriff auf E-Mail-, Kalender- und Kontaktdaten im Rahmen von Kommunikations- und Terminverwaltungsfunktionen. Die Datenverarbeitung erfolgt auf Grundlage eines abgeschlossenen Data Processing Addendum (DPA) mit Standardvertragsklauseln gemäss Art. 16 Abs. 2 lit. d DSG.
- **Pingen AG,** Schweiz – Versand von Rechnungsdokumenten in digitaler und physischer Form (Druck, Hybrid-Post). Die Verarbeitung erfolgt in der Schweiz; im Falle einer Drittlandweitergabe wird ein angemessener Datenschutz sichergestellt.
- **ServerBase AG**, Schweiz – Hosting und Bereitstellung von digitaler Infrastruktur (Servermanagement und IT-Dienstleistungen).
- **Infomaniak Network SA**, Schweiz – Bereitstellung von datenschutzkonformen KI-Dienstleistungen (KI-Sprachmodelle/Inference). Die Datenverarbeitung und Speicherung erfolgt ausschliesslich in den eigenen, ISO 27001 und ISO 50001 zertifizierten Rechenzentren von Infomaniak in der Schweiz. Eine Weitergabe von Daten an Drittstaaten oder Drittanbieter zu Trainingszwecken ist technisch und vertraglich ausgeschlossen.
- **Fullview ApS, Dänemark** – Bereitstellung von visuellen Support-Tools (Cobrowsing und Kunden-Support-Infrastruktur). Die Datenverarbeitung erfolgt DSGVO- und DSG-konform ausschliesslich auf Servern innerhalb der Europäischen Union (Region Frankfurt, Deutschland). Sensible Datenfelder werden systemseitig vor der Übertragung unkenntlich gemacht (Data Masking).